UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
v.	)	Criminal No. 09-10243-MLW
RYAN HARRIS	)	

GOVERNMENT'S OPPOSITION TO DEFENDANT'S MOTION FOR ACQUITTAL AND NEW TRIAL

From February 22 through March 1, 2012, during a trial that spanned almost two weeks, the jury in this case heard testimony from eight witnesses, including two TCNiSO insiders, two victim-experts, and three customers who successfully used Harris's products and services to steal internet service. The jury also considered documentary and video evidence that included business records, dozens of chat logs, web postings, book excerpts, and video clips.

Both before and during the trial, the defendant made numerous motions to dismiss each count of the indictment pursuant to Fed. R. Crim. P. 29, both on the merits and for lack of venue. The parties briefed and argued these motions extensively, often submitting multiple supplemental memoranda to the Court. The Court ultimately rejected all but one of the defendant's arguments. At the conclusion of the trial, the Court granted the defendant's motion to dismiss the sole § 371 conspiracy count (Count One in the original superseding indictment), essentially finding that there was insufficient evidence of a single conspiracy, rather than multiple conspiracies, because the government had not proven beyond a reasonable doubt that Harris's customers were interdependent with one another. The remaining eight substantive wire fraud counts were submitted to the jury.

On March 1, 2012, the jury returned a verdict convicting Harris of seven out of the eight counts of wire fraud charged in the indictment, in violation of 18 U.S.C. §§ 1343, 2.

The defendant now moves for judgment of acquittal and a new trial pursuant to Fed. R. Crim. P. 29(c)(1) and 33. As set forth below, the Court should deny both motions.

I. THERE WAS SUFFICIENT EVIDENCE TO ESTABLISH EACH ELEMENT OF WIRE FRAUD BEYOND A REASONABLE DOUBT

a. Legal Standards

i. Rule 29

In considering a challenge to the sufficiency of the evidence after trial, courts examine "whether any rational factfinder could have found that the evidence presented at trial, together with all reasonable inferences, viewed in the light most favorable to the government, established each element of the particular offense beyond a reasonable doubt." United States v. Richard, 234 F.3d 763, 767 (1st Cir. 2000) (quoting United States v. Gabriele, 63 F.3d 61, 67 (1st Cir. 1995)).

Courts have noted that a defendant "bears a heavy burden in arguing insufficiency of the evidence." United States v. Medina-Martinez, 396 F.3d 1, 5 (1st Cir. 2005). "A [district or] appellate court plays a very circumscribed role in gauging the sufficiency of the evidentiary foundation upon which a criminal conviction rests. The [district court or] Court of Appeals neither weighs the credibility of the witnesses nor attempts to assess whether the prosecution succeeded in eliminating every possible theory consistent with the defendant's innocence." Id. (citing United States v. Noah, 130 F.3d 490, 494 (1st Cir. 1997)). Courts "defer, within reason, to inferences formulated by the jury in the light of

its collective understanding of human behavior in the circumstances revealed by the evidence." Id. (citing United States v. Guerrero, 114 F.3d 332, 339 (1st Cir. 1997)). Accordingly, the Court's inquiry is only whether "the guilty verdict finds support in a 'plausible rendition of the record.'" Id. (citing and quoting United States v. Echeverri, 982 F.2d 675, 677 (1st Cir. 1993) and United States v. Ortiz, 966 F.2d 707, 711 (1st Cir. 1992)).[1]

Here, as set forth below, in considering both the direct and circumstantial evidence, and all plausible inferences drawn from it, and looking at the evidence in the "light most compatible with the verdict," it is clear that a rational jury could find beyond a reasonable doubt that Harris is guilty of committing the seven wire fraud counts of conviction.

ii. Wire Fraud Elements

As set forth in the defendant's memorandum, to prove wire fraud, the government must show (1) a scheme to defraud by means of false pretenses, (2) the defendant's knowing and willful participation in the scheme with the intent to defraud, and (3) the use of interstate wire communications in furtherance of the scheme. United States v. Casseire, 4 F.3d 1006, 1011 (1st Cir. 1993) (citations omitted). The falsehood must be

[1] Although the procedural posture of the cases cited above may have involved appeals, the standards for assessing the sufficiency of the evidence and for reviewing the denial of a Rule 29 determination are the same. Medina-Martinez, 396 F.3d at 5 (citing United States v. Hernandez, 218 F.3d 58, 64 n.4 (challenges to denial of Rule 29 motion and to sufficiency of evidence raise the same question)). See also United States v. Loder, 23 F.3d 586, 590 (1st Cir. 1994) ("This court reviews a district court's denial of a defendant's motion for a judgment of acquittal using the identical standard employed to measure the sufficiency of the evidence supporting a guilty verdict.") (internal quotation marks and citation omitted). Accord United States v. DiMasi, 810 F.Supp.2d 347, 351-52 (D.Mass. 2011) (echoing similar legal standard).

material. Neder v. United States, 527 U.S. 1, 16 (1999). The First Circuit has held that, in the context of a wire fraud charge, the government need not allege, let alone prove, that the defendant personally benefited from the fraud scheme. "It is immaterial whether [the defendant] personally profited from the scheme." United States v. Silvano, 812 F.2d 754, 758-62 (1st Cir. 1987). United States v. Vila, 2009 U.S. Dist. Lexis 2729 (D. PR. 2009). It is similarly well settled that a defendant can be convicted of wire fraud even when the scheme was never completed, no benefit accrued to anyone, and no loss ultimately took place. United States v. Potter, 463 F.3d 9, 17 (1st Cir. 2006); United States v. Louderman, 576 F.2d 1383, 1387 (9th Cir. 1978).

As set forth in the Court's jury instruction, in order to establish the use of the wires, "it is not necessary to prove that the defendant personally executed the [wires], but merely that the defendant 'caused the [wire communication] by doing some act from which it is reasonably foreseeable that the [wires] will be used.'" United States v. Bruckman, 874 F.2d 57, 60 (1st Cir. 1989) (quoting United States v. Gonzalez-Sanchez, 825 F.2d 572, 588 & n.54-55 (1st Cir. 1987)). As the Court also instructed the jury, to establish reasonable foreseeability, a defendant need not know anything about the particular wire charged; rather, it is merely the instrumentality of the wires that is the relevant inquiry. United States v. Pimental, 380 F.3d 575, 589-590 (1st Cir. 2005) (reversing district court on other grounds). "It is simply the 'use of the [wires or] mails' in the course of the scheme rather than the particular [wire or] mailing at issue that must be reasonably foreseeable for the causation element of a [wire or] mail fraud offense to be satisfied." Id. (citing Bruckman, 874 F.2d at 60 ("The causation element is met as long as some use of the mails was reasonably to be anticipated in the course of the

scheme"); United States v. Fermin-Castillo, 829 F.2d at 1198 ("As long as some use of the instrumentality in the course of the endeavor was reasonably to be anticipated, the causation requirement is met"); see also United States v. Bortnovsky, 879 F.2d 30, 38-39 (2d Cir. 1989) (noting that the causation element of mail fraud "has been so liberally construed as to suggest that it requires only that the use of the mail itself, rather than a particular mailing, be reasonably foreseeable" and endorsing that view).

b. Summary of Evidence Admitted at Trial

The evidence admitted at trial established beyond a reasonable doubt that Harris knowingly and willfully devised and participated in a scheme to defraud ISPs of subscriber revenues and network access, that the scheme involved material misrepresentations to the ISPs, and that the use of interstate wires was in furtherance of the scheme and reasonably foreseeable to Harris.

i. Harris's Scheme to Defraud ISPs

There was ample evidence presented at trial that, from 2003-2009, Harris ran a full-service and profitable "cable modem hacking" operation, providing everything users needed to successfully steal internet service from ISPs by masquerading as legitimate, paying subscribers. The technology Harris designed and used was described by Christopher Kohler, the Motorola witness, and Benjamin Brodfuhrer, the Charter witness, who also introduced video clips that recorded the results of his own product testing. In short, Harris and his customers would mimic or "clone" the cable modems of legitimate, paying subscribers to trick the ISPs into thinking that they were legitimate, paying

subscribers when they weren't.[2] They did this by "sniffing" for or otherwise acquiring subscriber account information called a Media Access Control ("MAC") address that belonged to legitimate, paying subscribers and then changing their modem's actual MAC address to the stolen MAC address.

Harris played a pivotal role in all of this. As the jury heard, Harris described himself as "the creator" and stated "I created the entire cable modem hacking scene." [Exhibits 17 and 21 (p.5)]. There was more than sufficient evidence, again through Harris's own statements, and corroborating insider testimony of his software programmer, Isabella Lindquist, and his roommate and business partner, Craig Phillips, that Harris, an avid gamer, was determined to steal cable internet service for himself, to become a millionaire by helping others steal cable internet service, and to punish the ISPs in the process. He put it succinctly in his "Hacking the Cable Modem" book, which was admitted into evidence. On his dedication page, he applauded "the righteous hackers that have been silenced by greedy corporations" and later wrote "my goal was clear: I wanted to uncap as many cable modems as possible! The war had begun." [Exhibit 7]. And his mission was to get rich by charging his soldiers money during the battle. As he told Phillips in chats, we are "on our path to becoming [sic] Millionairs [sic]" and "were [sic]

[2] As Kohler and Brodfuhrer testified at trial, a cable modem is a device that connects a computer to the coaxial cable wires that provide cable internet access to that computer. Each modem has a MAC address, which, like a serial number, is a theoretically unique identifier that manufacturers hard-code into the modems at the factory. ISPs use a modem's MAC address to determine if it belongs to a legitimate, paying subscriber. If the ISP recognizes the MAC address, the ISP then electronically sends a "configuration file" to the modem. The configuration file determines the speed and other parameters of the subscriber's internet service. ISPs typically charge premiums for faster internet service.

gonna make so much . . . money . . . and then were [sic] gonna buy a really nice house with a . . . . POOL . . .:D." [Exhibit 5, pp. 3, 16].

The insiders (Lindquist and Phillips), his customers, (Nathan Hanshaw, Jose LaRosa, and William Madeira), and the two victim-experts (Brodfuhrer and Kohler), each described pieces of Harris's full-service "cable modem hacking" operation. Through their testimony, as well as through other evidence, including video clips of Harris's products in use and screen shots of Harris's website, the jury heard ample evidence that Harris provided everything needed to steal service. He provided all the necessary equipment and the software to run it (including his self-styled "CoaxThief" MAC sniffing program), frequent software and hardware updates (such as "stealth mode," an anti-probing, and an anti-update feature), as well as access on his website to a steady supply of out-of-town stolen MAC addresses.

Harris also taught his customers how to use all of these tools. As the jury heard from the customer witnesses and saw on the screen shots of Harris's website, Harris posted video tutorials and instruction manuals on the website he created. He also ran something like an on-line help desk on his website, where he provided more instructions. As noted above, Harris wrote and sold a 250-page book, under his alias DerEngel, titled "Hacking the Cable Modem." [Exhibit 7]. In the end, as Phillips, Hanshaw, LaRosa, Madeira, and Brodfuhrer, all testified, all his customers had to do was attach Harris's equipment to their computer, input a stolen number from his website, his software, or elsewhere, and turn the modem on.

The evidence also established that the defendant stayed involved throughout. It was, as Phillips and Lindquist testified, Harris's full-time job. He kept very close track of

the providers' latest security measures and kept tweaking his "theft kit" in response. As Lindquist testified, Harris tried to stay one-step-ahead of the ISPs and played a game of "cat and mouse" with the ISPs. And as Brodfuhrer and Kohler testified, TCNiSO was a problem for the internet providers and the modem manufacturers, who worked hard trying to detect the defendant's customers and kick them off their network. When the providers or manufacturers released a new security measure to detect and block Harris's customers, as Lindquist testified, Harris would learn about it and instruct her to devise a new "work-around" to defeat it. Then, as Brodfuhrer, Kohler, and Lindquist testified, Harris would issue a new version of his tool kit, with updated software or hardware, including features like "Stealth Mode" and an anti-probing and anti-update feature.

Accordingly, in considering both the direct and circumstantial evidence, and all plausible inferences drawn from it, and looking at the evidence in the "light most compatible with the verdict," it is clear that a rational jury could find, beyond a reasonable doubt, that Harris devised or participated in a scheme to defraud the ISPs of subscriber revenues. See DiMasi, 810 F.Supp.2d at 351-52.

ii. Harris's knowing and willful conduct and intent to defraud

There was ample evidence that Harris knew full well about the scheme, willfully participated in it, and intended to defraud the ISPs. This includes (1) Harris's own statements about his intent to steal internet service for himself, become a millionaire by helping others steal service, and punish the ISPs in the process; (2) insider and co-conspirator testimony and Harris's own statements openly discussing uncapping and theft of service; (3) Harris's personal use of his own products to steal service; (4) the very

functionality of the products and services he offered; (5) Harris's continued involvement; and (6) Harris's attempts to hide and protect his users and himself.

1. Harris's Own Statements

As described above, the jury read chat logs, website posts, and book excerpts, and heard corroborating testimony from Phillips and Lindquist, that Harris was determined to devise a way to steal internet service for himself, to enhance his gaming experience, and to get rich helping others steal internet service for themselves. Indeed, business records were admitted into evidence showing that Harris grossed over $700,000 just from PayPal transactions, and only during a portion of the charged conspiracy. [Exhibit 30]. He also had a personal, and well-documented, vendetta against the ISPs, publicly declaring war on them in his book. [Exhibit 7].

2. Insider and Co-Conspirator Statements About Stealing Service and Fears of Getting Caught

Phillips, Harris's business partner and roommate, admitted that their entire operation was designed to help people steal free and faster internet service. He knew that virtually all of their clients were stealing free or faster service and that they were helping them do this. And he had conversations with the defendant openly discussing that their customers were stealing service and uncapping.

For example, evidence was admitted of at least two online conversations between Harris and Phillips and another co-conspirator where they openly discussed the fact that their customers were stealing (or at least planning on stealing) internet service and, in one conversation, that they would have to *teach* them how to steal.[3]

[3] Phillips told the defendant about a deal he was trying to put together to sell 10,000 copies of Harris's customized cable modem hacking software. Phillips said

Phillips and Lindquist both testified at trial that they very worried that what they were doing was illegal, they were worried about getting caught, and they openly discussed these fears with Harris.

Although Phillips was testifying pursuant to a cooperation plea agreement and Lindquist had been given court-ordered immunity, their testimony was corroborated by other evidence. In any case, in deciding a Rule 29 motion, the court may not "weigh the evidence or make any credibility judgments"; rather, credibility issues must be resolved in favor of the verdict. United States v. DiMasi, 810 F.Supp. 2d 357, 351-52 (D.Mass. 2011).

3. Harris's Personal Use of His Own Products to Steal Service

Phillips testified that he saw the defendant steal service before and while they lived together, that they obtained ten times faster service than beforehand, and that Harris taught Phillips how to use his products to steal service. Furthermore, they talked openly about it. In one chat between Harris and Phillips, Phillips is openly discussing the fact that he was stealing service. [Exhibit 5, p.1]. In another chat, Harris himself said that he was "getting free internet" [Exhibit 6, p.4]. There was also Harris's post on his own website forums looking for MAC addresses and promising rewards. [Exhibit 22].

---

explicitly to Harris: "they want to use these to steal service . . . we have to show them how to steal service too," and Harris doesn't flinch. He responded with: "sounds good to me" and suggests a price of $20k for the deal. He ends with "for 20K man, I'll give them UNLIMITED licenses." [Exhibit 5, p.14]. In another online chat, Mr. T, an unindicted co-conspirator, asked Harris if Sigma, his cable modem hacking product, was successfully "working 100% with all ISP?" and Harris replied that it worked with all but one, which they would have "cracked soon." [Exhibit 17, p.3].

4. The Nature of Harris's Products and Services

As Lindquist, Phillips, Brodfuhrer, and Kohler testified, Harris's products had two core functionalities: a MAC sniffer and a MAC changer. They also testified that the products had various functions to prevent ISPs from blocking and detecting users, including "stealth mode," an anti-probing function, and an anti-update function.

There was abundant testimony from Brodfuhrer and Kohler that Harris's theft kit had no commercially viable legitimate use. In essence, it was a single-use product designed to steal service. Brodfuhrer testified that there is no reason for an individual to sniff his neighbor's MAC addresses other than to steal service. Indeed, as the jury read in a chat between Harris and MooreR, Harris himself chose the name "CoaxThief" for his MAC sniffer. [Exhibit 21, p.4]. Phillips testified that he was not aware of a single purchaser who used the products as a diagnostic tool or for any other benign use.

Furthermore, to the extent that there could conceivably have been an ancillary benign use, that does not negate the overwhelming evidence of Harris's *intended* use, which is at issue in establishing that he committed wire fraud. Lindquist testified that Harris asked her to design a MAC changer, not a diagnostic tool, and he instructed her to design updates to get around ISPs' security measures. There was no testimony that Harris at any time directed Lindquist to design a diagnostic tool or privacy tool or "geek tinkerer" tool. Likewise, Phillips testified that offering unmodified modems for sale on the TCNiSO website was just a "cover."

There was also testimony that Harris operated (and used for himself) an online swap meet on his website, for customers to trade stolen MAC addresses and configuration files, and that he used it himself in an effort to obtain a MAC address. The jury also heard

testimony from Phillips and Hanshaw, both of whom personally and repeatedly used Harris's website to trade for stolen MAC addresses.

5. Harris's Continued Involvement

The government presented overwhelming evidence that the defendant did not merely design his cable modem hacking toolkit and walk away; he stayed very involved to make sure it worked properly. As noted above, the jury heard from Lindquist and the victim-experts that Harris monitored the ISPs security measures and played a "cat and mouse" game, in which he tweaked his products to make sure they defeated these measures.

In addition to the MAC swapping black market, Harris also ran a help desk on his website. Hanshaw and Lindquist both testified that they answered technical questions to help users operate the various products. Harris also posted video tutorials and written instructions on his website, [Exhibit 2], and the customer witnesses testified that they used these tutorials to help them steal service.

6. Harris's Attempts to Hide His Customers and Hide and Protect Himself

Lindquist, Brodfuhrer, and Kohler testified about functionalities in Harris's products that helped customers hide their identities, to make sure the ISPs couldn't detect them, including a feature that was called "stealth mode," as well as the anti-probing and anti-update features.

Harris also tried to hide himself. As the jury read, Harris admitted that he was paranoid and lived in hiding. In his "Hacking the Cable Modem" book, Harris wrote, "I make my living by pioneering hacking techniques . . . from my clandestine residence in Hong Kong." [Exhibit 7, "Introduction"]. As the jury also read, Harris said in an online

chat: "I'm a professional hacker [so I] get paranoid just to check who's at my front door." [Exhibit 21, p.5].

There was evidence not only of Harris's statements but also of his conduct. The evidence showed that Harris used the alias, DerEngel, whenever communicating about cable modem hacking. For example, as Special Agent Timothy Russell testified, nowhere on Harris's website did he ever use his actual name, Ryan Harris. He only used "DerEngel." The chats and website posts corroborated this testimony. Lindquist testified that she interacted with Harris almost daily online for over a year before he finally told her his real name, despite the fact that he was fully aware of her real name and address. As the jury saw with Harris book, [Exhibit 7], Harris wrote his book using his alias DerEngel, and although he put a photo of himself on his book, he references his alias in the caption of the photo. (Harris's name is mentioned one time in this 250-page book, in the fine print as the copyright owner). But he never used his real name when identifying who the author was or who the man in the photo was.

The evidence also established that Harris tried not only to hide himself but also to protect himself. He strategically placed "disclaimers" in some of his more public comments. But chats with Lindquist established that the defendant's so-called "disclaimers" were a joke. The insiders laughed about them. [Exhibit 6, p.3]. And Lindquist testified that they knew that their customers weren't following the disclaimers. Furthermore, as discussed above, the evidence established that Harris engaged in theft of service himself. In addition, as Phillips testified, and as various chats confirmed, Harris was eager to incorporate in California primarily as a method to protect himself legally.

Accordingly, in considering both the direct and circumstantial evidence, and all plausible inferences drawn from it, and looking at the evidence in the "light most compatible with the verdict," it is clear that a rational jury could find beyond a reasonable doubt that Harris knowingly and willfully participated in the scheme, with the intent to defraud. See DiMasi, 810 F.Supp.2d at 351-52.

iii. Reasonably foreseeable use of interstate wires in furtherance of scheme

The defendant does not take issue with the Court's jury instruction that "the use of the internet to send a message, such as an e-mail or a communication to a website, may be a wire communication." The evidence was overwhelming that Harris's operation, which spanned several years, was almost entirely web-based. As the insiders Phillips and Lindquist testified, and as the customers who acquired and used his products and tutorials confirmed, all product ordering was conducted through, and customer support was provided through, Harris's website. As Harris's own statements on his website confirmed, he sold at least 15,000 products. Accordingly, it was not only foreseeable, it was guaranteed, that his customers would be ordering his products using the wires. Furthermore, the very purpose of his fraud scheme was to steal internet service---which necessarily involves further use of the wires. Accordingly, it was not only foreseeable but again certain that his customers, when they used his products to steal service, would use the wires. Clearly, product ordering and product use to steal service were "in furtherance" of his scheme to defraud the ISPs of subscriber revenues and network access. Moreover, as Lindquist testified, Harris was determined to keep track of who was using his products at all times, apparently in an effort to prevent customers' from copying and distributing them without paying him. So he devised a registration license "key"

feature that required his customers to visit his website and enter their registration key in order to use his products. He also programmed a "phone home" technology so that his modems, when it use, would automatically have to visit Harris's website, pull down an invisible file from it, and in turn record the user's internet protocol address. This way, Harris could determine who his users were. Again, these registration and automated "phone home" features not only made the use of the wires reasonably foreseeable but guaranteed it.

As to the wires charged in counts one through four, Hanshaw testified that he acquired Harris's cable modem hacking products on two separate occasions, each time using the internet to do so. He also testified that he then used these products successfully to steal internet service. He testified about two online chat conversations he had with an individual who was located in Washington, while using Harris's products, both of which were admitted as Exhibits 11 and 12. As to Counts Five and Six, LaRosa testified that he acquired Harris's cable modem hacking products in 2008 by ordering them online from the TCNiSO website. He also testified that he then used these products successfully to steal internet service for approximately one to two years, starting in 2008. He stated that he repeatedly went back to the TCNiSO website to input his registration code, to view tutorials, to order products for himself, and approximately 20-25 times, he went back to the website to order products that he would then re-sell to a third party. LaRosa also testified that he exchanged several e-mails with the company trying to get replacement products. As to Count Seven, Madeira testified that he acquired Harris's cable modem hacking products in the summer of 2009 by ordering them online from the TCNiSO website.

Accordingly, in considering both the direct and circumstantial evidence, and all plausible inferences drawn from it, and looking at the evidence in the "light most compatible with the verdict," it is clear that a rational jury could find beyond a reasonable doubt that Harris could reasonably foresee the use of the wires and that these wire were in furtherance of his scheme to defraud the ISPs of subscriber revenues. See DiMasi, 810 F.Supp.2d at 351-52.

II. The Defendant's Arguments Lack Merit

a. The Defendant Misstates the Evidence

The defendant once again claims that the evidence at trial consisted "solely" of "product sales," "product capability," Harris's personal use, and known use. (Def's Memo p. 5-6). The defendant argues that this is insufficient for a jury to infer that Harris devised a scheme to defraud, intended to defraud, and participated in it with unknown users. As set forth in detail in above, the evidence at trial consisted of much more than this. There was abundant and uncontroverted evidence of Harris's *purposeful product design and intended use* (namely, to steal service by lying about one's identity), not simply "product capability" and "known use."

Again the defendant insists that the products had benign uses, echoing the very same arguments about "geek" tinkerers, privacy tools, and the like, made in his opening statement, in his closing argument, and throughout his witness cross examinations. Clearly, the jury rejected this argument. As discussed in more detail above, there was ample evidence to establish that Harris's self-styled "cable modem hacking" products ("CoaxThief," "stealth mode" and the like) were designed to, and in fact did, steal internet service.

b. The Defendant Misstates the Law

The defendant also argues, without support, that the government was required to prove, and failed to prove, that Harris participated in a scheme with each of his named users -- Hanshaw, LaRosa, and Madeira. (Def's Memo, pp. 7-8, 10). The defendant here apparently attempts to graft the elements of conspiracy onto the elements of wire fraud. But a defendant can be convicted of committing wire fraud by himself; he need not conspire with others. And in any case, here, there was ample evidence that Harris participated in a scheme to defraud the ISPs with the insiders Isabella Lindquist, Craig Phillips, and several other unindicted co-conspirators.

The government is not required to prove that Harris conspired with, or participated in a scheme with, each of his individual users. Not surprisingly, the defendant has cited to no authority for this point. In any case, Phillips testified that Harris had full knowledge of his customer records, often was in charge of shipping out products himself, and therefore a rational jury could infer that Harris knew the name and address and the products purchased by LaRosa and Madeira as well. Moreover, Lindquist testified that he kept track electronically of each of his users, by programming a "phone home" function into his products. In addition, LaRosa testified that he was not only a user but also a re-seller of Harris's products, he ordered dozens and dozens of products over the course of over a year, and he e-mailed back and forth with TCNiSO multiple times.

The defendant further challenges each of the individual wires. As to the counts relating to Hanshaw (Counts One-Four), Harris argues that the government was required to prove that Harris actually sold (rather than otherwise provided) his products to

Hanshaw. But a sale is not one of the elements of wire fraud. The defendant cites no authority for this requirement. His attempt to take, out of context, a sentence from one of the jury instructions regarding "what is not sufficient" is unavailing. Along those same lines, Harris argues that Harris "did not benefit in any way" from Hanshaw's conduct. (Def's Memo, p. 13). But the law is clear that Harris need not himself benefit financially from the wire fraud. United States v. Silvano, 812 F.2d 754, 758-62 (1st Cir. 1987). United States v. Vila, 2009 U.S. Dist. Lexis 2729 (D. PR. 2009). In any case, as set forth above, there was ample evidence that Harris's scheme to defraud ISPs was motivated in part by intent to punish (or, as he put it in his book, "declare war" against) the "greedy" ISPs, that is, by depriving them of subscriber revenues. A rational jury could infer that Hanshaw, by acquiring and then using Harris's products to steal internet service, was essentially a soldier in Harris's war, and his wires were made in furtherance of the scheme.

Harris then argues, again without authority, that the government was required to show precisely which version of Harris's various product offerings Hanshaw used to steal service. (Def's Memo, p. 12). Again, this misstates the law. As set forth above, the government need not prove that Harris's scheme to defraud the ISPs was ever completed or successful. United States v. Potter, 463 F.3d 9, 17 (1st Cir. 2006); United States v. Louderman, 576 F.2d 1383, 1387 (9th Cir. 1978). Thus, Harris's conviction would stand even if Hanshaw tried, but failed, to use Harris's products to steal service.

Further, the government need only prove that "the use of the wires" as an instrumentality was "reasonably foreseeable" to Harris. It need not prove that the

defendant knew of Harris's particular wires. United States v. Pimental, 380 F.3d 575, 589-590 (1st Cir. 2005).

As to the LaRosa and Madeira counts, Harris repeats many of the same arguments he made with respect to the Hanshaw wires, arguing that there was insufficient evidence that Harris conspired with LaRosa or Madeira, that LaRosa or Madeira used his products to steal service, and that Harris was aware of the particularities of LaRosa's or Madeira's wires. None of these arguments works, for the reasons set out above. Furthermore, LaRosa testified that, starting in 2008, he acquired a series of Harris's products and used them for one to two years successfully to steal service. He testified that he went back to Harris's website repeatedly, to register his own products, to acquire a series of additional products for himself, and on 20-25 separation occasions, he ordered more products for re-sale. He also sent multiple e-mails to the company. From this evidence, coupled with Lindquist's testimony that the products by themselves automatically "phoned home" to Harris's website when in use, a rational jury could reasonably conclude that the wires took place as charged in the indictment. To the extent the defense suggests that LaRosa may have continued using his neighbor's Wi-Fi during this period, there was no evidence of this.

c. The Defendant's Venue Challenge Lacks Merit

Peppered throughout Harris's memorandum are challenges to venue. The arguments lack merit. Venue is not an element of the offense, and the government bears the burden of proving it, not by a reasonable doubt, but merely by a preponderance of the evidence. United States v. Lanou, 137 F.3d 656, 661 (1st Cir. 1998) (citing United States v. Georgacarakos, 988 F.2d 1289, 1293 (1st Cir. 1993)). The venue determination should

be made "in the light most favorable to the government." Id. For an offense that is a "continuing" one, venue is proper "in any district in which such offense was begun, continued, or completed." 18 U.S.C. § 3237(a). "Begun" and "completed" are clear enough; the offense is continued if the wire transmission passes through facilities of interstate wire communication on its way from beginning to end. United States v. Carpenter, 405 F. Supp. 2d 85, 91 (D.Mass. 2005)(citing United States v. Pace, 314 F.3d 344, 349 (9th Cir. 2002); United States v. Goldberg, 830 F.2d 459, 465 (3d Cir. 1987).

Here, the parties stipulated to the fact that the TCNiSO computer servers were located outside of Massachusetts. The three customers who transmitted the wires at issue in each of the seven counts of conviction testified that they were living in Massachusetts when they used the internet to access the defendant's servers. Accordingly, viewing the evidence in the light most favorable to the government, there was a preponderance of evidence that venue in Massachusetts was proper.

III. A NEW TRIAL IS NOT WARRANTED

a. Legal Standard

The First Circuit has directed that the "remedy of a new trial [be] sparingly used, and then only where there would be a miscarriage of justice . . . and where the evidence preponderates heavily against the verdict." United States v. Indelicato, 611 F.2d 376, 387 (1st Cir. 1979) (quotation omitted). "When the district court considers a motion for new trial, however, it should interfere with the jury verdict only if the jury has reached a seriously erroneous result." United States v. Merlino, 592 F.3d 22, 26, n5 (1st Cir. 2010). "The remedy of a new trial is rarely used," and "merely reiterate[ing the] claim that the

evidence of intent was thin" does not warrant a new trial. United States v. Andrade, 94 F.3d 9, 14 (1st Cir. 1996).

b. References in Opening Statement to MAC Swapping Were Proper

Harris argues that the government improperly referred in its opening to Harris's operating a MAC swapping forum or "black market." He argues that "no evidence supported the claim" made in the opening statement that Harris operated a "black market" for trading stolen MAC addresses. This argument ignores the evidence admitted a trial. During the course of the trial, evidence was admitted that established that Harris, through his TCNiSO "forums" on his website, operated an online platform that allowed customers to trade, or otherwise obtain, stolen MAC addresses. Phillips and Hanshaw both testified that they used the TCNiSO forums to obtain stolen MAC addresses. A forum post made by Harris was admitted into evidence, where Harris was trying to obtain a MAC. [Ex. 22]. There was also testimony that Harris generally kept abreast of what was on the forums. Lindquist and Phillips both testified to that effect. That there were also other ways that a customer could obtain stolen MAC addresses does not negate the fact that Harris offered an online swap meet on his website, nor does it lessen the probative value of this evidence.

This evidence was relevant to both the substantive wire fraud charge, as well as to the conspiracy count that was later dismissed. The fact that Harris operated an online swap meet for trading out-of-town stolen MAC addresses was relevant to establishing Harris's scheme to defraud the ISPs and his knowing, willful, and intentional conduct. For example, it showed Harris's continued involvement in the enterprise, his "stake in the venture." The evidence also would negate the defendant's contention that he was selling

diagnostic tools and walking away, indifferent to how his customers were using his products. The existence of the "black market" on his website also was circumstantial evidence that Harris knew how his products were in fact being used. As Brodfuhrer testified, there is simply no legitimate reason to sniff for a neighbor's MAC address; likewise, a jury could infer that there is no legitimate reason to trade for stolen out-of-town MACs.

In any case, even if the evidence of the MAC swapping forum had not come in as anticipated, or had been only relevant to the conspiracy count that was dismissed at the conclusion of the trial, that is not a basis for granting a new trial. The defendant has cited no authority for this proposition. The First Circuit rejected a defendant's claim that an argument in support of a legal theory later found insufficient violated due process: "If it does not offend due process to affirm a conviction even though one of several charged theories of guilt had an insufficient evidentiary predicate..., *a fortiori*, mere argument in support of that insufficient legal theory, fairly derived from the record, cannot violate due process." United States v. Moran, 393 F.3d 1, 15 (1st Cir. 2004).

c. References in the Closing Argument and Rebuttal to the Lack of Evidence of the Purported Benign Uses Did Not Constitute Improper Burden Shifting

In his opening statement, in his closing argument, and throughout his cross examinations, Harris's counsel repeatedly argued that Harris's cable modem hacking products had a litany of benign uses, including as a privacy protection tool, a geek/tinkerer plaything, a diagnostic tool, a way to "get the speeds already paid for," and a way to enhance one's online experience by adjusting port access, filters, packet sizes,

and the like. Yet there was no evidence introduced that Harris's customers used his products for these purposes. It was wholly proper for the government to remark on this.

Remarking on this in no way amounts to improper burden-shifting. The First Circuit has held that where defendants had raised the possibility in opening statement and during cross-examination of a government witness that they had been "framed" by a confidential informant, government's closing argument was a "permissible comment on the weakness of the frame-up theory, and did not constitute prosecutorial misconduct" and that, "having put forth a theory in defense, a defendant cannot expect the government to refrain from commenting on its deficiencies." United States v. Lewis, 40 F.3d 1325, 1338 (1st Cir. 1994) (citing United States v. Glantz, 810 F.2d 316, 321 (1st Cir. 1987)).

These kinds of government arguments can create a burden-shifting problem when it is only the defendant who could, through his own testimony, establish his proffered defense. Here, however, the defendant himself would not have had to testify to establish his defense. Rather, other customers or insiders could have testified about how customers were in fact using Harris's products in benign ways. "Accordingly, the prosecutor's argument drew the jury's attention to what the evidence had shown, not to the defendant's decision not to testify." United States v. Bey, 188 F.3d 1, 7-8 (1st Cir. 1999) (holding that, to the extent that the defendant sought to contradict the matters that the government characterized as beyond question, he would not have had to rely on his own testimony; the evidence was within the competence of the other witnesses who testified at trial). United States v. Newton, 327 F.3d 17, 27 (1st Cir. 2003) (holding that rebuttal argument did not constitute an inappropriate comment on the defendant's failure to testify since defendant would not have had to rely on his own testimony to support his

defense; rather, that "would easily have been within the competence of other witnesses who could have testified at the trial. Hence, this is not a situation when contradiction of the government's case would have required the defendant to take the stand").

The First Circuit has stated that, "the government is entitled, to some extent, to comment on a defendant's failure to produce evidence supporting the defense theory of the case." Id. And to the extent that the government did this here, the Court specifically issued a cautionary instruction during the government's rebuttal, reminding the jury that the defendant did not have any burden to introduce evidence.

d. Admitting Evidence of Harris's Theft of Service Does Not Warrant a New Trial

As a threshold matter, challenging evidentiary rulings post-trial is not a basis for granting a new trial unless the jury "reached a seriously erroneous result." Merlino, 592 F.3d at 26, n5. Here, the Court properly admitted evidence of Harris's personal use of his own products to steal internet service, and in any case, irrespective of the ruling, there is ample evidence to support the jury's verdict.

This evidence does not, as the defendant contends, fall within the ambit of Fed. R. Evid. 404(b). First, it does not amount to evidence of "other" bad acts; rather, it is evidence of intrinsic bad acts that are part of the charged conduct. Although Harris was not charged with his own theft of service, he was charged with committing wire fraud, which included participating in and devising a scheme to defraud the ISPs by stealing service from them through material false pretenses. Initially, he was also charged with conspiring with others to commit wire fraud. Clearly, Harris's own theft of service, then, is an inherent part of his scheme to defraud the ISPs. Second, the evidence was not offered to show Harris's propensity to act in "conformity" with those prior acts. As the

defendant noted, Harris was not charged with theft of service in this case, so the fact that he stole service earlier on was not used to convict him of stealing service again at a later date.

Rather, the evidence of Harris's personal use was offered to show his intent and knowledge as it related to the scheme to defraud the ISPs. To the extent that Harris's defense was that he had no idea that his products could be used to steal internet service and never intended them to be used that way, the fact that he personally used them to steal service is highly probative of his state of mind.

IV. Conclusion

For these reasons, the Court should deny the defendant's motion for acquittal and for a new trial.

Respectfully submitted,

CARMEN M. ORTIZ
United States Attorney

By: */s/ Adam Bookbinder*
Adam J. Bookbinder
Assistant U.S. Attorney
Mona Sedky
DOJ Trial Attorney

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Adam Bookbinder

Dated: March 23, 2012